CONSIDERAZIONI SULLA φ DI EULERO

Giovanni Ferranti <gyofer@yahoo.it>

$\varphi(p) = p - 1$

$\varphi(p^n) = p^n - p^{n-1}$

$\varphi(n) = \varphi(p_1^{n_1} \cdot \ldots \cdot p_r^{n_2}) = \varphi(p_1^{n_1}) \ldots \cdot \varphi(p_r^{n_2})$

* * *

$x^{\varphi(m)} \equiv 1(m) \Leftrightarrow \begin{cases} (x,m) = 1 \\ 0 < x < m \\ x \in Z_m^* \end{cases}$ insieme elementi invertibili di Z_m.

$(x^{\varphi(m)})^b \equiv 1^b(m)$

$x^{\varphi(m)\cdot b} \equiv 1^b(m) \Rightarrow x^{\varphi(m)\cdot b} \equiv 1(m)$

quindi se $(x,m) = 1$ ed ho una congruenza del tipo:

$x^l \equiv 1(m)$ se $l = b \cdot \varphi(m)$

posso ridurla a $x^{\varphi(m)} \equiv 1(m)$.

(È come se facessi $\sqrt[b]{x^{b\cdot\varphi(m)}} \equiv \sqrt[b]{1}(m)$).

Inoltre se ho una congruenza:

$a^{\varphi(m)+b} \equiv x(m)$ con $(a,m) = 1$

$a^{\varphi(m)} \cdot a^b \equiv x(m)$

$a^{\varphi(m)} \equiv 1$

$a^b \equiv x(m)$ e così si è ridotto il grosso esponente della prima congruenza.

Infatti è come se facessi:

$[a^{\varphi(m)+b}]_m = [x]_m = [a^{\varphi(m)} \cdot a^b]_m = [a^{\varphi(m)}]_m \cdot [a^b]_m = [a^b]_m$

$[a^{\varphi(m)}]_m \equiv 1$ in Z_m essendo $(a,m) = 1$

Lo stesso vale se si ha:

$a^{n(\varphi(m)+b)} \equiv a^{n\cdot\varphi(m)+n\cdot b}$ ponendo nb=c

$\equiv a^{n\cdot\varphi(m)+c} \equiv x(m)$.

È come il caso precedente, stavolta con $n \cdot \varphi(m)$ invece di $\varphi(m)$.

È lo stesso, infatti, se $(a,m)=1$

$a^{n\cdot\varphi(m)+c} \equiv x(m)$

$a^{n\cdot\varphi(m)} \cdot a^{c} \equiv x(m)$

poichè $a^{n\cdot\varphi(m)} = \left(a^{\varphi(m)}\right)^{n} = 1^{n} = 1$ quindi $a^{c} \equiv x(m)$.
Si è così di nuovo ridotto la complessa congruenza iniziale ad alto esponente ad una più semplice con esponente più basso.

NOTA!! Ciò vale $\Leftrightarrow (a,m)=1$, condizione necessaria perchè $x^{\varphi(m)} \equiv 1(m)$ in Z_m.

Osservazioni: Se si ha $a^{n\cdot\varphi(m)} \equiv x(m)$ con $(a,m)=1$ è ovvio che x=1 in Z_m (cioè $x \equiv 1(m)$).
Infatti se n=0 si ha che $a^{0} \equiv x(m) \Rightarrow 1 \equiv x(m)$. In tutti gli altri casi si ha che $\left(a^{\varphi(m)}\right)^{n} \equiv x(m)$ cioè $1^{n} = 1 \equiv x(m)$ per Eulero.

NOTA!!! Non confondersi:

$a^{n\cdot\varphi(m)} = \left(a^{\varphi(m)}\right)^{n} \neq a^{\varphi(m)} \cdot a^{n}$. Per le proprietà delle potenze si ha che $a^{\varphi(m)} \cdot a^{n} = a^{\varphi(m)+n}$.